REMARKS

The Applicants wishes to thank the Examiner for the courtesies extended in the telephonic interview of 11/01/06. During the interview, the Examiner indicated the Applicant should file a response to the final Office Action reiterating arguments discussed during the interview.

Reconsideration and allowance in view of the following remarks are respectfully requested.

Claim 1-33 remain pending for examination.

The following remarks are responsive to the arguments presented in the Office Action of September 6th, 2006.

Rejections Under 35 U.S.C. §102(e)

Claims 12, 15, and **19** stand rejected under 35 U.S.C. §102(e) as being anticipated by Ala-Laurila (U.S. Patent 6,704,789; hereafter "Ala-Laurila"). The Applicant respectfully requests that this rejection be reconsidered and withdrawn. More particularly, the Applicant reiterates the arguments first presented in the response to the Office Action of 3/22/2006 that the rejection does not fulfill all of the requirements of MPEP §2131, which states, in part:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

In general, Ala-Laurila discloses using a subscriber identification module (SIM) to authenticate a user from a first network to a second data network. That is, Ala-Laurila is primarily directed to validating and identifying users consistently between a first network and a second data network. In contrast, **Claim 12** is directed, *inter alia*, to dynamically assigning internet protocol address to a wireless client over a secure link. In particular,

the authentication of a user and the establishment of one or more secure links are not analagous operations.

The rejection of **Claim 12** asserts that Ala-Laurila discloses receiving a request for a network address from the wireless client as "steps DHCP SOLICIT, figures 4 & 5". As discussed in the response to the Office Action of 3/22/2006, Ala-Laurila does not disclose the DHCP SOLICIT command. Ala-Laurila includes "Dynamic Host Configuration Protocol For IPv6 (DHCPv6) Work in Progress DHCP Working Group 1998, J. Bound and C. Perkins" by reference (*see* Ala-Laurila, col. 3, lines 27-29; hereafter "Bound and Perkins"). And, Bound and Perkins disclose the DHCPv6 command DHCP SOLICIT as sent by a client to locate a DHCPv6 server (*see* Bound and Perkins, Section 5.3. DHCP Message Types, "SOLICIT (1) A Client sends a solicit message to locate servers"). As discussed in the telephonic interview of 11/01/2006, **Claim 12** does not disclose receiving a request from a wireless client to locate a server; in contrast, **Claim 12** discloses receiving a request for a network address from the wireless client.

The rejection of **Claim 12**, first presented in the Office Action of 3/22/2006 maintains that Ala-Laurila discloses attaching information to the request to indicate that the request originated from a wireless client. The rejection maintains that a USER ID may include information to indicate the request originated from a wireless client. In addition, in the telephonic interview of 3/22/2006, the Examiner stated that the element of a USER ID was being given the broadest possible interpretation. However, during the interview the Applicant's representative reiterated that the USER ID is disclosed by Ala-Laurila at col. 5, lines 56-61 as follows:

> The smart card associated with the user terminal **12**, which may be of diverse designs, provides the user identification (USER ID) as described below in conjunction with FIGS. **4**-**6** and may be without limitation IMSI or NAI (Network Access Identifier) in accordance with RFC 2486.

More particularly, Ala-Laurila discloses that the user identification will be used to authenticate the user of a device but does not disclose the USER ID will be used for either authenticating or identifying devices. During the telephonic interview of 11/01/2006, the Applicant's representative reiterated the argument first presented in the response to the Office Action of 3/22/2006 that the USER ID Ala-Laurila is constant for the lifetime of the user identifier and that the user identifier does not change to reflect changes in the client device. Therefore, the user identifier as disclosed in Ala-Laurila does not change dynamically to indicate that a request originated from a wireless client as the rejection asserts. In contrast, **Claim** 12 does not disclose user information, user identification, or the like, let alone user information attached to a request. **Claim 12** only recites, *inter alia*, information indicating that the request originated from a wireless client. For example, see the specification of the application, page 10, lines 15-18:

> If the origin MAC address is in the database 203, the access point 202 modifies the discover packet at step 306 by inserting data into an optional field of the packet to indicate that the packet originated from a wireless client.

Furthermore, Ala-Laurila discloses the USER ID may be Network Access Identifier (NAI) in accordance with RFC 2486. As is known to those in the art, RFC 2486 discloses that a Network Access Identifier is of the form userid@realm. As can be seen, such a Network Access Identifier does not contain any information regarding whether or not the client request originated from a wireless device.

Therefore, for at least the reasons set forth above, it is respectfully submitted that **Claims 12, 15, and 19** are patentably distinguishable over Ala-Laurila. The present rejection under 35 U.S.C. §102(e) should be reconsidered and withdrawn.

Rejections Under 35 U.S.C. §102(b)

Claims 9, 11, 17, 21, 22, 24-27, 29 and 30 stand rejected under 35 U.S.C. §102(b) as being unpatentable over Lim et al. (U.S. Patent 5,884,024; hereafter "Lim"). The Applicant respectfully requests that this rejection be reconsidered and withdrawn. The Applicant reiterates the arguments presented in the response to the Office Action of 3/22/2006 that the rejection does not fulfill all of the requirements of MPEP §2131, which states, in part:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

The rejection of **Claims 9 and 21** reiterates that Lim discloses engaging in a negotiation of a secure link with the wireless client at column 7, lines 21-30. Column 7, lines 21-30 of Lim state:

> A preferred method for renewal of an IP address lease by DHCP server system **110** is shown in FIG. 7 and generally designated **700**. Method **700** begins with step **702** where DHCP server system **110** receives a broadcast DHCPREQUEST message from a client system **102**. For the purposes of illustration, it is assumed that the DHCPREQUEST message does not identify a specific DHCP server **110**. Thus, according to the DHCP protocol, the received message is a request from a client system **102** for renewal of an existing lease.

The Applicant wishes to reiterate the argument as originally presented in the response to the Office Action of 3/22/2006 that the cited section of Lim is generally directed to "a preferred method for renewal of an IP address lease by DHCP server system" and not to engaging in a negotiation of a secure link with the wireless client as in **Claims 9 and 21**. Furthermore, Lim is generally directed to extending the DHCP protocol to allow a server to check a database to determine whether the requestor of an address should be assigned an address. The DHCP server system of Lim is not configured to

manage links; rather, the DHCP server system of Lim is configured to, *inter alia*, assign internet protocol (IP) addresses to trusted clients and manage lease times and renewals for trusted clients.

And, as discussed in the telephonic interview of 11/01/2006, **Claims 9 and 21** are directed to a method for controlling access to a network over a secure link. For example, see the specification of the application, page 1, line 7, "a secure link, such as an IPSEC tunnel". As is known to those in the art, IPSEC is an industry standard set of protocols and services used to encrypt data transmission in an IP network. IPSEC is compatible with IPv4 and is included in IPv6. Lim is silent with regard to IPSEC, IPv4, and IPv6, and this is to be expected because, as discussed earlier, Lim is not directed to secure communication on a network.

The Applicant reiterates that engaging of negotiation of a secure link cannot be found either expressly or inherently in Lim. In addition, a wireless client also cannot be found either expressly or inherently in Lim. Therefore, it follows that the combination of engaging in a negotiation of a secure link with the wireless client cannot be found either expressly or inherently in Lim.

However, in the telephonic interview of 11/01/2006, the Examiner stated that the lack of a secure link and the lack of a wireless client within Lim are not grounds for patentability of **Claims 9 and 21** as Lim may be practiced over a wireless or a wired network. The Applicant's representatives disagreed and presented the argument that a wired connection may have different security requirements than a wireless connection. For example, data passing on a direct wire connection between two computer systems may be secure if there is no intermediary to intercept the data. However, data passing over a direct wireless connection between two computer systems may not be secure in the same scenario as the data is being broadcast through the air or another medium and any party that within receiving distance may be capable of intercepting the data.

Therefore, for at least the reasons set forth above and discussed with the Examiner in the telephonic interview of 11/01/2006, the Applicant reiterates that **Claims 9 and 21** are patentably distinguishable over Lim. Furthermore, **Claims 11 and 17** depend from **Claim 9** and are also patentably distinguishable over Lim for at least the same reasons as **Claim 9**. **Claims 22, 24-27, 29 and 30** depend from **Claim 21** and are also patentably distinguishable over Lim for at least the same reasons as **Claim 21**. The present rejection under 35 U.S.C. §103(a) should be reconsidered and withdrawn.

Rejections Under 35 U.S.C. §103(a)

Claims 1-8 and 31-33 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Nordman (U.S. Patent 6,061,346; hereafter "Nordman") in view of Garrett, *et al.* (U.S. 20020023160 A1; hereafter "Garrett"). The Applicant respectfully reiterates that the rejection fails to establish a *prima facie* case of obviousness, as set forth in MPEP §2143, which states, in part:

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

As previously presented in the response to the Office Action of 3/22/2006, Nordman is generally directed to a method for allowing a network-located device to access a private network by authenticating the network-located device in various ways. Furthermore, Garrett is generally directed to a method for managing the forwarding of network packets between networks managed by different service providers. In contrast, **Claim 1** is directed to assigning an address to a wireless client over a secure link using a wireless access point adapted to handle the secure link.

The arguments presented in the response to the Office Action of 3/22/2006 were reiterated by the Applicant's representatives in the telephonic interview of 11/01/2006. In particular, the Applicant does not agree that there is a suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the Nordman with the combination of Garrett (FIG. 9, steps 902-903 and step 904-906) for the stated purpose of allowing authorized use of an IP address and further enhance security of the system.

The Applicant's representatives reiterated the arguments first presented in the response to the Office Action of 3/22/2006 that the system of Nordman already includes security, for example, the title of Nordman is "Secure Access Method, and Associated Apparatus, for Accessing A Private IP Network". It is not clear why one of ordinary skill in the art would be motivated to combine Garrett to provide the enhancement of security when a primary concern of Nordman is a secure access method. That is, the "Radius Server 930" from FIG. 9 of Garrett may not be combined with Nordman, as Nordman already includes a "DHCP Server 920" from Garrett. The "RADIUS Server 930" from FIG. 9 of Garrett is defined in Garrett at paragraph 36 as follows:

> Alternatively, the DHCP server 161 in the service activation system 160 can interact with the registration server 155 using a back-end authentication protocol, e.g. the Remote An Authentication Dial In User Service (RADIUS). See C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication Dial In User Service (RADIUS)," IETF Network Working Group, RFC 2058 (January 1997), which is incorporated by reference herein. The DHCP server can contain a RADIUS client and, thereby, leverage the large RADIUS embedded base used for dial access authentication.
>
> ...
>
> The DHCP server 920 forwards both the challenge and response in a RADIUS_ACCESS_REQ message to a RADIUS server 930 in the selected service network. The

> RADIUS server 930 either accepts or rejects the RADIUS request and responds accordingly at 906. If the RADIUS request is accepted, the DHCP server 920 sends a DHCPACK message at 907 and the client 910 enters a bound state. If the RADIUS request is rejected, the DHCP server 920 sends a DHCPNACK message which informs the client 910 that the IP address that was allocated has been withdrawn.

The RADIUS Server 930 of Garrett is defined as server providing remote authentication dial in user service. As RFC 2058 has been incorporated by reference into Garrett, RADIUS servers are defined in RFC 2058 at "section 1: Introduction" as follows:

> RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

Nordman already includes such functionality in the form of the Home Location Register (HLR) (*see* Nordman, column 6, lines 55-62, "The HLR 76 includes an authentication center"). Therefore, it is not clear what additional security benefit there would be to including a RADIUS Server of Garrett to Nordman, as Nordman is already capable of providing exactly the same security functionality with the Home Location Register. Therefore, there is no motivation to combine Nordman with Garrett as there is not a case of *prima facie* case of obviousness, as set forth in MPEP §2143.

The Applicant respectfully maintains that neither Nordman nor Garrett, either singularly or in combination, teaches or suggests the features of independent **Claim 1** or corresponding dependent **Claims 2-8, and 31-33**. The Applicant submits that **Claims 2-8 and 31-33** are patentably distinguishable over the proposed combination of Nordman and Garrett for at least the reasons set forth above due to their dependency upon independent **Claim 1**.

Accordingly, for at least the reasons set forth above, it is respectfully submitted that a *prima facie* case of obviousness has not been established for any of the presently

rejected claims. Therefore the present rejection under 35 U.S.C. §103(a) should be reconsidered and withdrawn.

CONCLUSION

All objections and rejections having been addressed, it is respectfully submitted that the present application is now in condition for allowance. Early and forthright issuance of a Notice of Allowability is respectfully requested.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an enclosed check please charge any deficiency to Deposit Account No. 50-0463.

Respectfully submitted,

Microsoft Corporation

Date: 11/6/06

By: _____

Carole A. Boelitz, Reg. No.: 48,958
Attorney for Applicants
Peter Taylor
Direct telephone: (425)722-6035
Microsoft Corporation
One Microsoft Way
Redmond WA 98052-6399

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being electronically deposited with the USPTO via EFS-Web on the date shown below:

November 6, 2006
Date

_____
Signature

Kate Marochkina
Type or Print Name